

Defendant's Exhibit A

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

19-CR-103-JLS-HKS

v.

AFFIDAVIT

SHANE GUAY,

Defendant.

STATE OF NEW YORK)
COUNTY OF ERIE) ss:
CITY OF BUFFALO)

SHANE GUAY , being duly sworn, deposes and states:

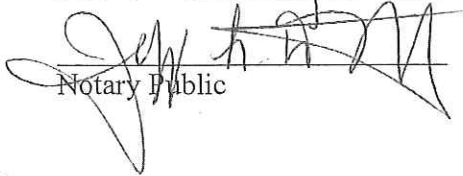
1. I am the defendant in this matter and I make this affidavit in relation to the suppression motion filed by my attorney, Jeffrey T. Bagley, Assistant Federal Public Defender.
2. This affidavit is based upon my personal knowledge.
3. I have not set forth all the facts known to me in this affidavit – only those I believe are necessary to establish standing.
4. I live at 147 North 8th Street, Olean, New York in Cattaraugus County and did so when the search in this case was conducted. I have at all relevant times considered it my home and have had keys to this residence, and thus I enjoyed an expectation of privacy there.

5. Inside my residence are several of my possessions. This includes: an LG G6 cell phone; an Acer Laptop Aspire One; a Compaq Presario Tower; a Dell Inspiron laptop; and an LG G4 cellphone. All these items were seized when the search was conducted. At the time these items were seized, I enjoyed an expectation of privacy in each of these items.

DATED, this the 21 day of January, 20 20.

Sworn to before me this

21st day of January, 20 20


Notary Public

JENNIFER L. DIMITROFF
Notary Public, State of New York
Qualified in Erie County
Commission Expires April 16 2023


SHANE GUAY

Defendant's Exhibit B

APPLICATION FOR SEARCH WARRANT
(Section 690.35 CPL)

STATE OF NEW YORK
LOCAL CRIMINAL COURT

COUNTY OF CATTARAUGUS
CITY OF OLEAN

To the Presiding Justice, Hon. Daniel Palumbo, City of Olean, Cattaraugus County, NY:

A) IN THE MATTER OF AN APPLICATION:

1. I, Investigator Daniel J. Walsh, a Police Officer in the State of New York employed by the New York State Police, do hereby apply for a search warrant pursuant to the provisions of Article 690 of the New York State Criminal Procedure Law. Pursuant to this request, I hereby state that there is reasonable cause to believe that property, of a kind or character described in Section 690.10 of the New York State Criminal Procedure Law, will be found in or upon a designated or described place, vehicle or person.

B) DESCRIPTION OF THE PERSON AND PLACE TO BE SEARCHED:

1. The person of **SHANE M. GUAY** d.o.b. 05/04/1991, wherever he may be found and The residence at **147 NORTH 8TH STREET, OLEAN, NY 14760 – CATTARAUGUS COUNTY.**

2. The place to be searched is described as a two story, two family residence. The residence is located on the West side of North 8th Street and is approximately 200 feet South of the intersection of Washington Street, in the City of Olean, Cattaraugus County, New York. The front of the house faces East, towards North 8th. The house number, "147", is attached above the front door, which is located on the covered front porch on the East side of the house. The residence has gray siding on the house. The residence is further identified in the image below:

Note: There is a driveway on the South side of the house, that leads to a smaller covered porch on the South side of the house. The house number, "145", is attached above the door, located on the smaller covered porch on the South side of the house. This entrance and corresponding living area are **NOT** included in the Application and Search Warrant.



3. Your applicant requests authorization to enter and search, the aforementioned residence, in addition to any other areas the residents have custody and/or control over on the property. The search may include the basement, attic, an unattached garage, shed, barn and vehicles located within the curtilage of the property.

C) THE PROPERTY SOUGHT TO BE SEIZED, EXAMINED AND/OR HELD:

1. Your applicant requests authorization to search for, seize, examine and retain, the following property located upon the person and at the place to be searched listed under section "B":

a) **COMPUTERS** - As this term is defined in New York State Penal Law Section 156.00. "Computers" include, but are not limited to, desktop computers, laptop computers, computer servers, tablet computers, netbook computers, notebook computers, cellular telephones, digital video recorders, video surveillance systems and/or video gaming systems. Specifically, your applicant is requesting to search for, examine and seize any "computer" that may contain evidence of or may have been used to commit any of the following crimes: Use and/or Attempted use of a child in a sexual performance (Penal Law 263.05) and/or Promotion or Attempted Promotion of a sexual performance by a child (Penal Law 263.15) and/or Possession or Attempted Possession of a sexual performance by a child (Penal Law 263.16) and/or Disseminating indecent material to minors in the second degree (Penal Law 235.21(3)) and/or Endangering the welfare of a child (Penal Law 260.10 (1)).

b) **COMPUTER PERIPHERAL DEVICES** - A computer "peripheral" device is defined as any device that can be attached to a computer in order to expand its functionality. Computer peripheral devices include, but are not limited to, keyboards, mice, routers, modems, scanners, video display units, video cameras, web cams, transfer and/or power cables and their internal and/or external data storage devices. Specifically, your applicant is requesting to search for, examine and seize any "peripheral" device that may contain evidence of or may have been used to commit any of the following crimes: Use or Attempted use of a child in a sexual performance (Penal Law 263.05) and/or Promotion or Attempted Promotion of a sexual performance by a child (Penal Law 263.15) and/or Possession or Attempted Possession of a sexual performance by a child (Penal Law 263.16) and/or Disseminating indecent material to minors in the second degree (Penal Law 235.21(3)) and/or Endangering the welfare of a child (Penal Law 260.10 (1)).

c) **COMPUTER DATA STORAGE DEVICES** - A computer data "storage" device is defined as a device used for the purpose of storing computer data. Computer data storage devices include, but are not limited to, hard disk drives, floppy disks, compact disks, digital video disks, magnetic tapes, flash drives, memory cards, media cards, zip drives and RAM and/or ROM units. Specifically, your applicant is requesting to search for, examine and seize any "computer data storage device" that may contain evidence of or may have been used to commit any of the following crimes: Use or Attempted use of a child in a sexual performance (Penal Law 263.05) and/or Promotion or Attempted Promotion of a sexual performance by a child (Penal Law 263.15) and/or Possession or Attempted Possession of a sexual performance by a child (Penal Law 263.16) and/or Disseminating indecent material to minors in the second degree (Penal Law 235.21(3)) and/or Endangering the welfare of a child (Penal Law 260.10 (1)).

d) **COMPUTER SECURITY DEVICES** - A computer "security" device is defined as a physical device, password, computer software, computer data and/or associated documentation that is used, or may be used, to restrict access to, or hide, computer data or computer software. Computer data security devices may consist of hardware, software and/or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software, or code, may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it. Specifically, your

applicant is requesting to search for, examine and seize any computer security device that may have been used to conceal any of the following crimes: Use or Attempted use of a child in a sexual performance (Penal Law 263.05) and/or Promotion or Attempted Promotion of a sexual performance by a child (Penal Law 263.15) and/or Possession or Attempted Possession of a sexual performance by a child (Penal Law 263.16) and/or Disseminating indecent material to minors in the second degree (Penal Law 235.21(3)) and/or Endangering the welfare of a child (Penal Law 260.10 (1)).

e) **RECORDS AND/OR DOCUMENTS** – Any personal papers, written or printed documentation, and/or computer data, which identifies the owner, users or other parties having custody or control over the premises or items being searched for and/or seized.

1. Any written or printed documents that contain Child Erotica.

f) **COMPUTER DATA** – Whether stored internally within a computer system itself and/or externally within an external computer data storage device (e.g. hard drive, floppy disk, compact disk, digital video disk, flash drive, memory card), your applicant requests permission to search for and seize any computer data which constitutes evidence of and/or aids in identifying any victims of any of the following crimes: Use or Attempted use of a child in a sexual performance (Penal Law 263.05) and/or Promotion or Attempted Promotion of a sexual performance by a child (Penal Law 263.15) and/or Possession or Attempted Possession of a sexual performance by a child (Penal Law 263.16) and/or Disseminating indecent material to minors in the second degree (Penal Law 235.21(3)) and/or Endangering the welfare of a child (Penal Law 260.10 (1)). Specifically, your applicant requests that the search may include, but is not limited to, the following computer data:

1. Image and/or video files containing suspected sexual performances by children, as defined in New York State Penal Law Sections 263.00.

2. Records of Internet web sites visited.

Web site history can be used to show that a specific computer was used to access a web site or service such as Instagram and/or may provide evidence related to the identity of the perpetrator of the crime and/or the identity of the user/owner of the item being examined.

3. Records containing a computer user's keyword searches.

Keyword searches, i.e. Google searches, can be used to show that a computer user knowingly and intentionally searched for images and/or videos containing sexual performances by children and/or searched for intended victims. Keyword searches may also provide evidence related to the identity of the perpetrator of the crime and/or the identity of the user/owner of the item being examined.

4. Records containing a computer user's communication content and/or history. This may be in the form of e-mail, chat, SMS (Text), MMS (Multi-Media Message), and/or video messaging. These messages can be used to show that a computer user knowingly and intentionally possessed and/or promoted images containing sexual performances by children by their conversations with other like-minded individuals. These Records may also show information regarding any Victims, which may include communications and Images and/or Video. Records containing a computer user's communication content and/or history may also provide evidence related to the identity of the perpetrator of the crime and/or the identity of the user/owner of the item being examined.

5. Records containing phone numbers, user names, e-mail addresses, address or contact

books and/or internet account screen names. These records can be used to show that a computer user accessed a web site or service such as Instagram and/or may provide evidence related to the identity of the perpetrator of the crime and/or the identity of the user/owner of the item being examined.

6. Evidence of the existence or absence of any malware that could have been used to illegally upload or download images and/or videos containing sexual performances by children to or from a seized computer or computer data storage device.

7. Image files and/or video files and/or other Data that contains Child Erotica.

8. Computer file metadata. Metadata contains information about the computer data files on a computer. This includes, but is not limited to, GPS coordinates of where an image was created, dates and/or times a file was created, last modified or accessed, file size, etc. This information may provide evidence related to the investigation or the identity of the perpetrator of the crime.

9. Device Settings - Any computer data which tends to identify the settings and/or identification of the device being searched (e.g. device phone number, serial number, battery level, applications installed, etc). This information is needed to document the specific device being examined, how the device was being used and/or where evidence of the crime being investigated may be stored.

10. Location Records - Any computer data containing location data related to the crime being investigated. (e.g. - GPS coordinates, location address, etc).

11. Images and/or Videos - Image files and/or video files that are visually similar to the images sent by and contained within the suspect Instagram account and/or Image files and/or video files of any Victim(s) and/or Image files and/or video files that may provide evidence related to the identity of the perpetrator of the crime and/or the identity of the user/owner of the item being examined.

g) ANY CELLULAR TELEPHONE, OR MOBILE DEVICE PRESENTLY OR PREVIOUSLY IDENTIFIED BY ONE OR MORE OF THE FOLLOWING:

1. Mobile Directory Number (MDN), also known as the "Telephone" number or "Cell" number of 716-307-1305.
2. International Mobile Equipment Identity/Identifier (IMEI) of 357903066270590.

h) SPECIFIC IDENTIFIABLE LOCATIONS WITHIN A RESIDENCE OR BUILDING

Specifically, your applicant is requesting to search for, photograph and otherwise document any locations within the place to be searched listed under section "B", that appear to be visually identical or similar to images that were described in section D(4)(a) and D(8)(a) of this search warrant application.

D) ALLEGATIONS OF FACT TO SUPPORT REASONABLE CAUSE:

1. I, Daniel J. Walsh am the applicant herein and serve as a public servant, of the kind specified in New York State CPL Section 690.05 (1). I am a police officer, employed by the New York State Police since June 28, 2004. I am currently employed as an Investigator in the Bureau of Criminal Investigation assigned to the SP Olean Station. I have completed 26 weeks of training, at the New York State Police Academy, which included instruction in conducting criminal investigations. I have been involved in many investigations related to the sexual abuse of children, possession and/or promotion of sexual performances by children and investigations involving the use of computers for criminal purposes. I am aware of the methods used by individuals to illegally possess and/or promote images containing sexual performances by children, in violation of the New York State Penal Law Article 263.00. I am also familiar with the tools that said individuals commonly use commit these crimes, including the use of computers and the Internet network.

Investigator John Lombardi is a public servant, of the kind specified in New York State CPL Section 690.05 (1). He is a police officer, employed by the New York State Police since 1989. Investigator Lombardi has been assigned to the New York State Police Computer Crime Unit since 2008. Investigator Lombardi is also a member of the Internet Crimes Against Children Task Force which investigates the sexual exploitation of children via the Internet. Investigator Lombardi has been involved in hundreds of investigations related to the sexual abuse of children, the endangerment of children, possession and promotion of sexual performances by children and investigations involving the use of computers for criminal purposes. He has received over 500 hours of training, by the New York State Police and other agencies, in the investigation of computer related crimes and the search, seizure and examination of digital evidence.

2. In support of my assertion as to the existence of reasonable cause, the following facts are based upon the statement of others, who have personal knowledge, and/or upon the personal knowledge, training and/or experience of other police officers and/or myself. Any fact provided will include the source of that information. Because this application is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish reasonable cause.

3. There is reasonable cause to believe that certain property, described above under Section "C", will be found on the Person and/or at the location to be searched. The property is:

a) Believed to have been used to commit an offense against the laws of this state, in violation of Article 263 of the New York State Penal Law; and

b) Constitutes evidence and/or tends to demonstrate that an offense was committed in this state, in violation of Article 263 of the New York State Penal Law.

c) Furthermore, some of the property (i.e. a sexual performance by a child) is unlawfully possessed.

4. This investigation is based upon a Law Enforcement Referral from Detective Olivia Siekman of the Shirley, Massachusetts Police Department. The referred case (Shirley Police Department

Incident [REDACTED] was based upon online communications directed to multiple juvenile females from **INSTAGRAM** usernames/IDs "**heythereitsme56**" and "**helloimboored100**" via direct message. The Juvenile females were all 11 or 12 years old at the time of the incident. A summary of what Detective Siekman reported is detailed as follows:

a) Between November 6, 2016 and November 7, 2016, Instagram account "**heythereitsme56**" direct messaged multiple Juvenile students, including a juvenile identified as [REDACTED] (DOB [REDACTED]) and sent an image to them, which Detective Siekman described as follows:

"It consisted of the lower half of a white male (possibly between the ages of 18 to 30 years of age, post pubescent) holding an erect penis with his left hand. The male was lying down in a room that had wood paneling on the walls and posters. There appeared to be a dark purple blanket hanging from a door way."

b) One of the Juveniles identified as [REDACTED] (DOB [REDACTED]) received multiple text based direct messages between November 6, 2016 and November 7, 2016, a few of which are:

"Hey sexy"

"Can you send a pic please."

"Do it in private...please. We can keep it a secret"

"Please babe you have a pic of you that your vagina is showing through your yoga pants. It's so hot. Do you shave your vagina?"

"Would you like me licking your vagina and rubbing it till you get so wet and cum"

"I wish you were into this so I could trade naked pics with you"

c) Similar messages were also sent to the other juveniles, but more lengthy messages were sent to [REDACTED] (DOB [REDACTED]).

d) Between November 7, 2016 and November 8, 2016 Instagram account "**helloimboored100**" sent direct messages to some of the juveniles. The juvenile identified as [REDACTED] (DOB [REDACTED]) was addressed directly by her first name and received multiple text based direct messages, a few of which are:

"[NAME]...just answer me please."

"I'll leave you alone if you send a pic."

"Just a pic."

"1 pic"

"It's not hard."

"It's easy"

e) Between November 7, 2016 and November 8, 2016 Instagram account "**helloimboored100**" direct messaged TWO images to the juvenile identified as [REDACTED] (DOB [REDACTED]). The first image showed a female, with her legs spread apart, exposing her vagina. The included message said, "Can I do this to you?" The second image showed a penis penetrating a vagina.

f) It is noted that Detective Olivia Siekman indicated that this incident was also being investigated by the Ayer, Massachusetts Police Department, as there were additional complainants in their jurisdiction that are not listed in the following affidavit. Refer to attachment 2 - affidavit of Detective Olivia Siekman of the Shirley, Massachusetts Police

Department. (Corresponds to Facebook Search Warrant application)

5. On December 07, 2016, pursuant to a Search Warrant issued by the Ayer Division, Massachusetts District Court, Facebook/Instagram provided records and account content to Detective Olivia Siekman for the following accounts for the Date Range 11/05/16 at 00:00:00 UTC through 11/08/16 at 23:59:59 UTC:

- a) Instagram User name "**heythereitsme56**" with Instagram User ID number 4121932649.
- b) Instagram User name "**helloimboored100**" with Instagram User ID number 4121932649.

Instagram further reported the following information regarding Instagram User names "**heythereitsme56**" and "**helloimboored100**" with Instagram User ID number 4121932649.

- c) The Instagram User ID number for both "**heythereitsme56**" and "**helloimboored100**" is **4121932649**.
- d) The Instagram account identified by User ID number "**4121932649**" was created/registered on 11/05/16 at 23:08:51 UTC from IP Address 2600:1017:b114:3d54:fc00:6f10:3e0d:677c. The Registered E-mail address for Instagram account identified by User ID number "**4121932649**" is **shaneg1991@gmail.com**.
- e) The User name/Vanity name, "**heythereitsme56**" had a first name of "george" listed.
- f) The User name/Vanity name, "**helloimboored100**" had a first name of "ash" listed.
- g) From 11/05/16 at 23:08:51 UTC through 11/08/16 at 22:57:36 UTC, there were a total of 179 login events from 8 different IPV6 addresses and 1 login event from one IPV4 address.
- h) The last login event occurred on 11/08/16 at 22:57:36 UTC from IP Address 2600:1017:b129:8929:5c32:bb20:794f:87e6.

6. From 12/13/16 to 3/13/17, Detective Siekman reported that the Facebook/Instagram search warrant results contained an identifiable picture of a male's face that had a background that appeared to be the same as the background of the picture of the male's erect penis that was described in section D(4)(a) of this document. Detective Siekman also discovered that [REDACTED] (DOB [REDACTED]) was Facebook friends with a Facebook profile of "**SHANE GUAY**" that used the same image of the male's face that was seen in Facebook/Instagram the search warrant results. Detective Siekman further reported that "**SHANE GUAY**" lived in Olean, NY and is a distant relative of a friend of [REDACTED]'s mother.

7. On 05/01/17, Investigator John Lombardi received Case materials and data, including the Facebook/Instagram search warrant content that had been forwarded by Detective Olivia Siekman of the Shirley, Massachusetts Police Department.

8. On 05/01/17 and 05/02/17, Investigator Lombardi reviewed the Case materials and data, including the Facebook/Instagram search warrant content. Investigator Lombardi made the following observations:

- a) In addition to screen captures of the images previously described by Detective Siekman, the case data included a digital image of a person believed to be "**SHANE GUAY**" that is described as follows:
The image shows a shirtless white male standing in front of a medium stained wooden door in what appears to be a light-colored tiled bathroom, with a distinctive black tile accent/border. There is also what appears to be a tan patterned shower curtain visible in the image. The male has short dark hair, with thick eyebrows, a beard and moustache. He has a light skin tone, with

moderate to heavy, dark colored arm and chest hair. In the center of his chest is a tattoo of a red heart, with what appears to be a noose around it. On his stomach, towards the left side of the image, the top part of a tattoo depicting what appears to be the animated character of "Jack Skellington". It is noted that the image may be reversed as this digital image appears to have been a "selfie", taken in the mirror.

- b) The Facebook/Instagram search warrant data for the Instagram account identified by User ID number "4121932649" contained numerous Direct Messaging text and images that were both sent and received by the two account User names/Vanity names "heythereitsme56" and "helloimboared100". The actions contained in this account appear to be concentrated on sexual conversations and obtaining images and/or video of clothed and unclothed girls and female genitalia. It appears that some of the activity detailed by Detective Siekman was no longer present in the account at the time of the search warrant. Additionally, the following observations were made:

- 1) On 11/07/16 at 19:50:54 UTC, an Instagram user with the same name as [REDACTED] (DOB [REDACTED]) sent a direct message to "heythereitsme56" that said "Stop".
- 2) On 11/08/16 Instagram user "helloimboared100" had numerous Direct Messaging communications with Instagram user [REDACTED]. Based on the conversation and non-contraband images sent by [REDACTED], the user presented as a female, who appeared to be from 15 to 18 years of age. In this conversation, "helloimboared100" presented as a 12 year old female.
 - a) On 11/08/16 at 13:53:56 UTC, Instagram user, "helloimboared100" sent an image of an erect penis to Instagram user [REDACTED]. This image matched the description of the image described by Detective Seikman in section D(4)(a) of this document. It is also noted that this image was visually identical to the same image in screen captures of Instagram messages contained in the case data forwarded by Detective Seikman.
 - b) On 11/08/16 at 13:58:41 UTC, Instagram user, "helloimboared100" sent an image of a Female to Instagram user [REDACTED]. The image is described as an image of the upper torso and head of a white female with medium complexion, who appears to be under the age of 14 years old. The child has long brown hair. The child has a gray bra on that is pulled down, exposing her nipples and slightly developed breasts.
 - c) On 11/08/16 at 13:59:08 UTC, Instagram user, "helloimboared100" sent an image of a Female to Instagram user [REDACTED]. The image is believed to be the same child, who appears to be under the age of 14 years old, as the one seen in the previous image. The image shows the child turned to her left, showing mostly a profile of her right side, angled to show a little of the front of her body. The child's body is visible from below the shoulders to just below the top of her hips. The child is leaning forward, with her back arched and her shoulders upright. The gray bra is pulled down, exposing her right nipple and part of both breasts. Her left hand is laying flat on her lower abdomen and pubic region, with her fingers extended down towards her vagina. The placement of her left hand can give the appearance that the child is either masturbating or covering her genitals.

- d) On 11/08/16 at 14:34:06 UTC, in response to the question "How old are you" from Instagram user [REDACTED], Instagram user, "helloimboored100" responded with "12...:/".
- e) On 11/08/16 at 20:36:46 UTC, Instagram user, "helloimboored100" sent a closeup image of a vagina to Instagram user [REDACTED]. The image is a closeup of a vagina that shows part of the right inner thigh and stomach of the female. The right fingers and thumb of the female are being used to spread open the vagina. The skin tone of the female is similar to the skin tone of the child, who was described in the previous two images. There is no pubic hair visible. The approximate age or identity of the female cannot be determined from this image. This image was the 3rd of three closeups of what is believed to be the same vagina that were sent by "helloimboored100". The context of the conversation indicated that the three images, were images of the vagina of the 12 year old that was presented by "helloimboored100".
- 3) On 11/08/16 Instagram user "helloimboored100" had numerous Direct Messaging communications with Instagram user [REDACTED]. Based on the conversation and non-contraband images sent by [REDACTED] the user presented as a female child that identified herself as "10" years old. Images posted by [REDACTED] showed a female child, who appeared to be under the age of 12 years old. In this conversation, "helloimboored100" originally identified himself as a 13 year old male. Later in the conversation "helloimboored100" sent images of the Torso and Face of the person believed to be "SHANE GUAY" and identified them as images of himself, "helloimboored100".
- a) On 11/08/16 at 16:54:06, Instagram user, "helloimboored100" sent an image of an erect penis to Instagram user [REDACTED]. This image matched the description of the image described by Detective Seikman in section D(4)(a) of this document. It is also noted that this image was visually identical to the same image in screen captures of Instagram messages contained in the case data forwarded by Detective Seikman.
- b) On 11/08/16 at 16:54:57 UTC, in response to the question "So do you like this?" from Instagram user "helloimboored100", Instagram user, [REDACTED] responded and said "no im only 10!!!!".
- c) On 11/08/16 at 17:08:35 UTC, in response to the question "...how old are u" from Instagram user [REDACTED], Instagram user, "helloimboored100" responded with "13".
- d) On 11/08/16 at 17:40:26 UTC, after asking Instagram user [REDACTED] multiple times for pictures, Instagram user "helloimboored100" said "Hmm I wish you could just show me something sexy...pretty please. It can be our secret. I'll do anything you want."
- e) On 11/08/16 at 22:42:22 UTC, after asking Instagram user [REDACTED] multiple times to use her phone to masturbate, Instagram user "helloimboored100" said "So just walk to your kitchen and tell me go, then slide your phone down your pants and then hold it against your vagina. 20 seconds. Pretty please."

- f) On 11/08/16 at 23:16:07, after asking "Would you want to see my body?", Instagram user, "helloimboored100" sent an image of a shirtless upper torso of a male to [REDACTED]. The torso shown, matched the description of the image believed to be "Shane Guay" previously described by Investigator Lombardi in section D(8)(a) of this document. Both Tattoos previously described were visible in the image and "helloimboored100" identified the tattoo of "Jack Skellington" in his messages to [REDACTED].
- g) On 11/08/16 at 23:18:03, Instagram user, "helloimboored100" sent an image of the Face of a male believed to be "Shane Guay" to [REDACTED]. The image showed a male with short dark hair, thick eyebrows, a beard and moustache. He has a light skin tone. The background of the image appeared to be the same background as seen in the picture of the male's erect penis, described by Detective Seikman in section D(4)(a) and previously sent to Instagram user [REDACTED]. Prior to sending the "Face" picture, "helloimboored100" made references to being "Fat" and "Ugly". After receiving the "Face" picture of "helloimboored100", [REDACTED] replied "Ur not ugly". "helloimboored100" replied "Well thank you. But I think I am."

9. On 05/01/17 Investigator Lombardi located a Facebook Profile for a "Shane Guay". It was observed to be an established Facebook page with numerous pictures(selfies) of a male believed to be "Shane Guay", who listed "Holiday Valley Ski Resort in Ellicottville" as his place of employment. Investigator Lombardi observed that the profile picture for "Shane Guay" was visually identical to the picture of the male's face that was sent from "helloimboored100" to [REDACTED] on 11/08/16 at 23:18:03 UTC and described in section D(8)(b)(3)(g) of this document. He also observed that this same picture was posted to the Facebook photos section of "Shane Guay's" profile on July 21, 2016. Investigator Lombardi compared this Facebook profile picture of "Shane Guay" to the picture of the Male's penis that was sent by "heythereitsme56" to [REDACTED] (DOB [REDACTED]) and other juvenile victims between 11/06/16 and 11/07/16. Investigator Lombardi stated that it was his belief that both pictures were taken at the same location, based on the following background similarities:

- a) Brown wall paneling with dark vertical lines was visible in both images.
- b) An unidentified poster on the wall with similar patterns and coloring was visible in both images.
- c) Visible in both images is, blue fabric which is hanging vertically over what appears to be a doorway or opening in the paneling. The bottom of the fabric is stringy and appears to be shredded.
- d) In the image of the male's face believed to be "Shane Guay", it appears that a New England Patriots poster is hanging on the blue fabric. In the image of the male's penis, the background is slightly blurry, but the bottom corner of what appears to be a poster is visible, hanging on the blue fabric.
- e) A light colored light switch cover that is on the wall between the blue fabric and the unidentified wall poster is seen in both images.
- f) Investigator Lombardi observed that left and right were reversed in the images, which is not uncommon with some "selfies".

10. On 05/01/17, while viewing the Facebook photos section of "**Shane Guay's**" profile, Investigator Lombardi observed a photo (selfie) of a male believed to be Shane Guay that appears to have been taken in the same a light-colored tiled bathroom, with a distinctive black tile accent/border that was observed in the image showing "**Shane Guay's**" tattoos, described in section D(8)(a) of this application. It was also observed that this image was posted to Facebook on 10/10/12.

11. On 05/02/17 – Investigator John Lombardi, conducted a check of New York State Department of Motor Vehicles and ascertained that "**Shane M. Guay**", DOB 05/04/91 has a valid driver's license, with an address of **147 NORTH 8TH STREET, OLEAN, NY 14760**. Investigator Lombardi also obtained the driver's license photo of "**Shane Guay**" from the NYS DMV. After comparing the two photos, Investigator John Lombardi confirmed that it was his belief that the white male observed in the Facebook profile photo of "**Shane Guay**", as well as in the other images believed to be "**Shane Guay**" was the same person identified as "**Shane Guay**" in the NYS DMV photo.

12. A check of the Arin.net internet database reported that each of the 8 different IPV6 addresses, and the 1 one IPV4 address reported by Facebook/Instagram for the suspect account with Instagram User ID number 4121932649, are controlled by VERIZON Wireless. On September 5, 2017, pursuant to a subpoena, VERIZON wireless reported that:

- a) On 11/05/16 at 23:08:51 UTC, IPv6 address **2600:1017:b114:3d54:fc00:6f10:3e0d:677c** and on 11/08/16 at 22:57:36 UTC, IPv6 address **2600:1017:b129:8929:5c32:bb20:794f:87e6** were assigned to Mobile Telephone Number **716-307-1305**, under the Billing Account in the name of CAROL LATA at **150 NORTH 8TH STREET, OLEAN, NY 14760**.
- b) A sample of 24 additional login dates and times across the 8 different IPv6 addresses were subpoenaed and were also reported to be assigned to Mobile Telephone Number **716-307-1305**, under the Billing Account in the name of CAROL LATA at **150 NORTH 8TH STREET, OLEAN, NY 14760**.
- c) For the 1 IPv4 address, "NAT" routing was in use. VERIZON reported that on 11/07/16 at 12:51:44 UTC, IPv4 address 70.195.136.221 was in use by 128 different subscribers/Mobile Telephone Numbers, including Mobile Telephone Number **716-307-1305**.
- d) The effective activation date for Mobile Telephone Number **716-307-1305**, under the Billing Account in the name of CAROL LATA was 01/28/08.

13. On September 28, 2017, Investigator Lombardi conducted a Facebook Search for Carol Lata and located a profile for "Carol Abdo Lata". Investigator Lombardi observed a photo, that was posted on 02/18/17, that had the comment "7 of my grandchildren!". It was noted that the male believed to be "**Shane Guay**" was in picture.

14. On September 28, 2017, Investigator Lombardi conducted a Facebook Search for Cellular Phone Number **716-307-1305**. The Facebook search results indicated that the Cellular telephone number **716-307-1305** is associated with the Facebook profile identified by the name "**Shane Guay**". Investigator Lombardi confirmed that this is the same "**Shane Guay**" profile he previously described. Additionally, Investigator Lombardi observed that "**Shane Guay**" and "Carol Abdo Lata" were Facebook friends.

15. On November 14, 2017, pursuant to a subpoena requesting additional information regarding Mobile Telephone Number **716-307-1305**, for the period from 11/01/16 through 10/27/17, VERIZON wireless reported that:

- a) The Mobile device had an International Mobile Equipment Identity (IMEI) of 357903066270590.
- b) One of the active features indicated the mobile phone can be used as a Mobile Hotspot.
- c) Verizon also provided Text and Call detail records.

16. On March 29, 2018, Investigator Lombardi again conducted a Facebook Search for Cellular Phone Number **716-307-1305**. The Facebook search results indicated that the Cellular telephone number **716-307-1305** was still associated with the Facebook profile identified by the name "**Shane Guay**". Investigator Lombardi confirmed that this is the same "**Shane Guay**" profile he previously described.

17. On April 6, 2018, Investigator Lombardi further reviewed the Facebook profile identified by the name "**Shane Guay**". While viewing the Facebook photos section of "Shane Guay's" profile, Investigator Lombardi observed a photo (selfie) of a male believed to be Shane Guay that appears to have been taken in the same a light-colored tiled bathroom, with a distinctive black tile accent/border that was previously, described in sections D(8)(a) and D910) of this application. It was also observed that this image was posted to Facebook on March 24, 2018.

18. On April 06, 2018, Investigator Lombardi conducted a search of New York State Police Spectrum Justice System database, which contains New York State Police Incident reports and other information. Records indicated that a "**Shane M. Guay**", DOB 05/04/91 was interviewed by Trooper David Fisher on May 23, 2013. His reported address at that time was **147 NORTH 8TH STREET, OLEAN, NY 14760**. His reported phone number at that time was **716-307-1305**.

19. On April 06, 2018, Investigator John Lombardi, conducted a check of New York State Department of Motor Vehicles and ascertained that "**Carol A. Lata**", DOB [REDACTED] has a valid driver's license, with an address of **150 NORTH 8TH STREET, OLEAN, NY 14760**.

20. On April 04, 2018, Investigator John Lombardi, conducted a check of New York State Department of Motor Vehicles and confirmed that "**Shane M. Guay**", DOB 05/04/91 still has a valid driver's license, with an address of **147 NORTH 8TH STREET, OLEAN, NY 14760**.

21. On April 15, 2018, I conducted a records check at OLEAN PD. Officer [REDACTED] confirmed they have dealt with SHANE M. GUAY on multiple occasions dating back to 2008. On all occasions SHANE M. GUAY has provided a home address of 147 N. 8th Street, Olean, NY 14760.

22. On May 24, 2018, I interviewed [REDACTED] the resident of [REDACTED] [REDACTED] confirmed SHANE M. GUAY is a current resident of 147 N 8th St. Olean NY.

23. Based upon the information cited in this section, my knowledge and/or experience and upon consultation with Investigator John Lombardi, there is reasonable cause to believe that between 11/05/16 at 00:00:00 UTC and 11/08/16 at 23:59:59 UTC, The Instagram account, represented by Instagram User ID number 4121932649, displayed/used Instagram User name "**heythereitsme56**" and then Instagram User name "**helloimboored100**". There is also reasonable cause to believe that during this period, this account was created by and repeatedly accessed, by a user, using the Cellular Telephone or Mobile Device bearing Verizon Wireless Cellular Telephone Number **716-307-1305**.

24. Based upon the information cited in this section, my knowledge and/or experience and upon consultation with Investigator John Lombardi, there is reasonable cause to believe that from November 6, 2016 through November 8, 2016, a user, using the Instagram account, represented by Instagram User ID number 4121932649 and Instagram User names "**heythereitsme56**" and "**helloimboored100**" sent images of a male's penis to multiple juvenile females and attempted to obtain images of 1 or more juvenile female's vaginas, in violation of New York State Penal Law 263.05, 263.15, 263.16, 235.21(3) and 260.10 (1).

25. Based upon the information cited in this section, my knowledge and/or experience and upon consultation with Investigator John Lombardi, there is reasonable cause to believe that on 11/08/16 at 20:36:46 UTC, an Instagram user, using the Instagram account, represented by Instagram User ID number 4121932649 and Instagram User name "**helloimboored100**" sent a closeup image of a hairless vagina to another Instagram user, while representing that the vagina in the image, was that of a 12 year old, in violation of New York State Penal Law 263.15 and 263.16.

26. Based upon the information cited in this section, my knowledge and/or experience and upon consultation with Investigator John Lombardi, there is reasonable cause to believe that multiple factors indicate that "**Shane M. Guay**", DOB 05/04/91 is a user of the Verizon Wireless Cellular Telephone Number **716-307-1305**. Some of these factors include Law enforcement contact with "**Shane Guay**", where the New York State Police and the City of Olean Police Department recorded this number as a contact for "**Shane M. Guay**". An additional factor is the association of this phone number with "**Shane Guay's**" Facebook profile.

27. Based upon the information cited in this section, my knowledge and/or experience and upon consultation with Investigator John Lombardi, there is reasonable cause to believe that multiple factors indicate that "**Shane M. Guay**", DOB 05/04/91 is the user and/or has knowledge of the user of the Instagram account, represented by Instagram User ID number 4121932649 and Instagram User names "**heythereitsme56**" and "**helloimboored100**". Some of these factors include the multiple images of "**Shane M. Guay**" within the suspect account, the fact that the background of the suspect image of a Male's penis appears to be the same background as "**Shane Guay's**" Facebook profile image and that the suspect Instagram account was created and repeatedly accessed by a user, using the Cellular Telephone or Mobile Device bearing Verizon Wireless Cellular Telephone Number **716-307-1305**, which is known to be associated with "**Shane Guay**".

28. Based upon the information cited in this section, my knowledge and/or experience and upon consultation with Investigator John Lombardi, there is reasonable cause to believe that multiple factors indicate that from 2008 to present, "**Shane M. Guay**", DOB 05/04/91 has resided at and/or listed his residence as **147 NORTH 8TH STREET, OLEAN, NY 14760**. Some of these factors include Law enforcement contact with "**Shane Guay**", where the New York State Police and the City of Olean

Police Department recorded **147 NORTH 8TH STREET, OLEAN, NY 14760** as the address for "**Shane M. Guay**", DOB 05/04/91. The New York state Department of Motor Vehicles has **147 NORTH 8TH STREET, OLEAN, NY 14760** listed as "**Shane Guay's**" address. Additionally, a neighbor acknowledged that "**Shane Guay**" currently lives at **147 NORTH 8TH STREET, OLEAN, NY 14760**.

29. Based upon the information cited in this section, my knowledge and/or experience and upon consultation with Investigator John Lombardi, there is reasonable cause to believe that a Cellular Telephone or Mobile Device bearing Verizon Wireless Cellular Telephone Number **716-307-1305**, will be found upon the person of and/or in proximity to and/or at the residence of "**Shane M. Guay**", DOB 05/04/91. Based on other factors in this investigation as well the tendencies and behaviors of persons who demonstrate a sexual interest in children and commit violations of New York State Penal Law sections, 263.05, 263.15, 263.16, 235.21(3) and 260.10 (1), there is also reasonable cause to believe that additional evidence relevant to the investigation and/or bearing evidence of violations of New York State Penal Law sections, 263.05, 263.15, 263.16, 235.21(3) and 260.10 (1), may be found upon the person of and/or in proximity to and/or at the residence of **Shane M. Guay**", DOB 05/04/91, residing at **147 NORTH 8TH STREET, OLEAN, NY 14760**.

E) COMPUTERS AND CHILD PORNOGRAPHY

1. Based upon my knowledge, training and/or experience, and upon consultation with Investigator John Lombardi, of the New York State Police Internet Crimes Against Children Task Force, I know that:

a) Images of sexual performances by children are not readily available in U.S. retail establishments. Accordingly, individuals who wish to obtain images of sexual performances by children usually do so by photographing child victims themselves, intentionally visiting Internet web sites that sell or provide the images and/or by making discreet contact with other individuals who trade sexual performances by children on the Internet via e-mail, instant messaging, peer to peer networks and/or by other computer software applications such as Tumblr.

b) The Internet has become the preferred avenue for promoting, trading and/or collecting images of sexual performances by children. An individual, familiar with a computer and the Internet, can easily use said tools in the privacy of their own home or office to interact with other like-minded individuals located anywhere in the world. The use of a computer provides an individual, interested in sexual performances by children, with a sense of privacy and secrecy that is not attainable by other traditional methods of transmission like postal mail. It also gives an individual a method of immediate gratification by having the ability to immediately view images and/or videos that have been acquired from others.

c) Individuals involved in the possession and/or promotion of images of sexual performances by children tend to retain the images for long periods of time. Those individuals, interested in images of sexual performances by children, prize the images they obtain, trade and/or sell. In addition to their "emotional" value, the images are valuable as trading and/or selling material and therefore are rarely destroyed or deleted by the individual collector.

d) Some of the more common methods used by individuals to promote, trade and/or obtain images of sexual performances by children, from other like-minded individuals, include the use of peer to peer networks, e-mail and/or instant messaging programs on a computer. It is also common for persons, who are interested in collecting images of sexual performances by children, to store their collection on removable media such as memory cards, CD's, DVD's, external hard drives, cellular phone memory and in remote storage accounts created on Internet web sites like Google, Photobucket, Dropbox and YouTube. The remote storage and removable media methods provide these individuals with the belief that they are limiting their risk of detection by law enforcement, family and/or friends, by not storing their collection on shared computers.

e) Computer data, including images containing sexual performances by children, can be stored on a computer's hard drive, in a computer's memory "RAM" and/or in other digital media storage devices including, but not limited to, MP3 players, cellular phones, digital cameras and video game systems. Storing computer data can be intentional (i.e. saving an e-mail as a file on the computer's hard drive or saving the location of your favorite websites in bookmarked files). Computer data can also be retained unintentionally on a computer's hard drive, memory and/or on digital media storage devices (i.e. A user's Internet activity is usually recorded in the web cache and history files on a computer's hard drive). A computer examiner can often recover this and other valuable evidence, years later. Such information may also be maintained indefinitely until overwritten by other data.

f) Individuals involved in the possession, and/or promotion of images of sexual performances by children, also tend to possess materials containing Child Erotica. Child Erotica as defined in attachment 1(Definitions) of this document is not necessarily a violation of State and/or Federal Laws and therefore may be more readily available to individuals who wish to obtain it. While there are both paid and free websites containing Child Erotica, an individual can easily obtain material constituting Child Erotica through simple internet searches. The presence of Child Erotica tends to demonstrate that an individual has a sexual interest in children and tends to provide supporting evidence of an individual's knowledge and intent in cases such as this one.

g) Individuals involved in the possession, and/or promotion of images and/or videos of sexual performances by children have sometimes been found to possess magnetic media tapes (VHS, 8MM, Mini-DV Etc.) containing Video recordings that constitute a sexual performance by a child.

F) ONLINE SOCIAL NETWORKING AND PREDATORY BEHAVIOR

Based upon your affiant's knowledge and experience and upon the knowledge, training and experience of Investigator John Lombardi, who your affiant consulted with prior to completing this search warrant application, your affiant knows that there are numerous Online Social Networking sites and Applications which facilitate communication and file transfers between individuals and groups. I also know that Individuals who exhibit Predatory Behavior towards Children and/or Minors use Online Social Networking Sites and Applications as follows :

1. Individuals often use social networking sites and applications such as Facebook, Instagram, KIK, Etc. to meet and/or communicate with other persons they are interested in having a social and/or sexual relationship with. Certain individuals identified as Predators often use social networking sites to meet and/or communicate with children and/or minors that they are interested in having a physical

and/or social sexual relationship with.. In many cases, using one or more Social networking profiles/user accounts, these individuals communicate with several children and/or minors at the same time in order to increase their chances of locating children and/or minors that they can have a physical and/or social sexual relationship with.

2. Predatory Individuals will often use fictitious profiles/personas in order to hide their true identity and to be more appealing to their intended targets. This allows them to appear to have common interests and circumstances with their intended targets in order to facilitate further contact and gain the trust of their targets.

3. Predatory Individuals will often use multiple profiles/personas to communicate with a single child or minor. This conduct allows them to gather more information about their intended target and tailor subsequent profiles/personas in order to increase familiarity, bonding and trust with their intended target. They will often use one profile/persona to introduce another profile/persona to their intended target. It is also common for them to use multiple profiles to exert peer pressure, such as all of the profiles saying and demonstrating that they often share/send naked pictures/videos of "themselves". Predatory individuals will also send naked pictures/videos to desensitize their intended target, so they are more likely to send naked pictures back.

4. It is common for predatory individuals to attempt to convince children and minors to send or share naked pictures and/or videos of themselves that would constitute a sexual performance by a child. Predatory individuals will often start with requests for less invasive or revealing images/video and continue request more invasive, revealing and sexual images/video each time the child or minor complies. It is not uncommon for predatory individuals to successfully coerce children and minors by threatening to send previously obtained images/video to the child's friends and/or family if the child refuses to send them additional and increasingly sexually explicit photos/video.

5. It is common for predatory individuals to possess multiple images and/or videos that would constitute a sexual performance by a child and/or child erotica. These images and/or video may be from children that they victimized online, or they may be images and/or video obtained from other sources. It is also common for predatory individuals to send these images and/or videos to their intended targets.

G) COMPUTERS, DATA STORAGE DEVICES AND DIGITAL EVIDENCE

Based upon my knowledge, training and/or experience, and upon the knowledge, training and experience of Investigator John Lombardi, who your affiant consulted with prior to completing this search warrant application, your affiant knows that:

1. Computers and Data Storage Devices, routinely contain valuable digital evidence. The possible forms and types of data that could be considered valuable digital evidence are too numerous to completely list. Every single computer file has the potential to be of value in a case such as this. The file name, file dates and times and the file content of each file could potentially constitute the evidence being sought in this case.

2. Some, but not all of the more common types of valuable digital evidence that may be found on computers and data storage devices that could reasonably contain evidence being sought in this case are:

a) Image files and Video files which could contain:

- 1) Images or video of users or owners of the item being examined, which may aid in determining who was using the item being examined as well as where and when the item was being used.
- 2) Images or video of specific locations, persons or items that may be pertinent to this case. This information could possibly identify perpetrators, victims and criminal associates.
- 3) Images and/or Video of sexual performances by children and/or child erotica.
- 4) Metadata or Exif Data that may be pertinent to this case.

b) Data files and document files which could contain personal identifying information of any users or owners of the item being examined, including but not limited to Software registration files, Hardware registration files, credit card records, and online purchase receipts.

c) Communications data which could contain identifying information of any users or owners of the item being examined including but not limited to E-mail, Instant messages, Call Logs, Contact Lists/Address Books and Social Media posts (Such as Facebook). In cases such as this, it is reasonable to believe that Communications data may also contain correspondence with victims, associates and/or persons or entities that knowingly or unknowingly participated in the commission of a crime.

d) Internet History and data which could contain identifying information of any users or owners of the item being examined as well as locations pertinent to this investigation including but not limited to screen names, websites visited and map/direction searches.

e) GPS (Global positioning system) data which may contain location information, trip information, and addresses of previous destinations as well as stored destinations. This data may aid in the identification of users and/or owners.

H)

CELLULAR TELEPHONES AND DIGITAL EVIDENCE

Based upon my knowledge, training and/or experience, and upon the knowledge, training and experience of Investigator John Lombardi, who your affiant consulted with prior to completing this search warrant application, your affiant knows that:

1. Cellular or Mobile devices and any attached memory and/or SIM cards, routinely contain valuable digital evidence. This evidence may consist of, but is not limited to, call history (i.e. received calls, dialed calls, and missed calls), Short Message System (SMS) messages,

Multimedia Message System (MMS) messages, pictures, videos, phone book information, Internet history, e-mail, documents and/or calendar events, device settings, user names and/or identity, call history, contacts and/or address books, calendar events, stored communications, images and/or videos, security codes, Internet history, installed applications, location records and possibly malware.

2. Many users will also program their Cellular telephones with personal information to identify themselves as the owner of a particular device.

3. Many Cellular telephones today also function as GPS units, which may additionally store location information, trip information and addresses of previous destinations as well as stored destinations.

4. Many Cellular telephones and mobile devices can function as a "Wireless hotspot", which will allow other computers and devices to connect to the internet via the subscribed data plan for that cellular telephone or wireless device. This connection can also be completed via a USB cable and is called "tethering". In either of these cases, any computer or device connected to the internet through a cellular subscriber's data plan, would be connecting to the internet through an IP address assigned to the Cellular service/carrier.

5. Cellular telephones routinely store digital information or potential evidence by use of Read Only Memory (ROM), Random Access Memory (RAM), as well as removable media (Data Storage Device) such as memory cards and/or Subscriber Information Module (SIM) cards.

6. The definition of "Computer" (Penal Law 156.00) also encompasses Cellular Telephones as it describes the basic functions of virtually all Cellular Telephones in use presently.

7. Most Cellular Telephones allow additional software or computer programs, commonly known as applications or "apps" to be installed.

8. Many Cellular telephone users now use their telephone in the same manner as a traditional desktop or laptop computer is used. Cell phone users often use their phones to access the internet and browse web sites, send and receive E-mail and access personal files and data that are stored on the cell phone or at another location as well as use the various forms of internet based communication and social media such as Facebook, Instagram, KIK, Etc.

9. Evidence (in the form of computer data), including but not limited to call history, Short Message System (SMS) messages, Multimedia Message System (MMS) messages, pictures, videos, phone book information, Internet history, e-mail, documents and/or calendar events, can be knowingly or unknowingly saved on cellular phone memory or a data storage device. An example of when computer data is stored intentionally may include the act of saving an image as a file on your Cell Phone or saving the location of your favorite websites in, for example, "bookmarked" files. Computer data can also be retained unintentionally on cellular phone memory and/or on a data storage device. For example, Internet activities are generally automatically recorded in the Internet history files on a Cellular Telephone, without the knowledge of some Cellular Telephone users.

10. Most Cellular telephones in use today can also function as a digital camera, digital video recorder and digital audio recorder.

11. It is common for users to transfer data from older cell phones to newer cell phones, when they upgrade or switch devices. Users can backup/preserve, maintain and transfer/restore this data by various methods, including but not limited to Cloud based backup as well as applications that backup data to a local computer or storage device. Because of a user's tendency to value their data and the ease of which this data can be transferred to a new device, it is now common to see data on a user's current device, that also is and/or was present on a previously used device.

12. A forensic examiner can often recover digital evidence and other evidence from cellular telephones and data storage devices, years later. Such information, even if it had been previously deleted may also be maintained indefinitely and therefore recoverable until overwritten by other data.

I) **IDENTIFICATION OF CELLULAR AND MOBILE DEVICES**

Based upon your affiant's knowledge and experience and upon the knowledge, training and experience of Investigator John Lombardi, who your affiant consulted with prior to completing this search warrant application, your affiant knows that:

1. There are multiple unique identifiers that may be associated with a Cellular or Mobile device. Some of the identifiers are permanently associated with a specific device and some identifiers are "portable" and can be "transferred" to another device. The following identifiers are some, but not all off the possible identifiers that may be found on a cellular or Mobile device. Each cellular or mobile device does not necessarily support or contain every type of identifier.
 - a) Mobile Directory Number (MDN), also known as the "Telephone" number or "Cell" number.
 - b) International Mobile Subscriber Identity (IMSI).
 - c) International Mobile Equipment Identity (IMEI).
 - d) Mobile Equipment Identifier (MEID).
 - e) Mobile Station Identification Number (MSID).
 - f) Electronic Serial Number (ESN).

J) **SEIZURE OF DIGITAL EVIDENCE**

1. Based upon my knowledge, training and/or experience, and upon consultation with Investigator John Lombardi, a computer forensic examiner with the New York State Police Computer Crime Unit, I know that:

- a) Searching and seizing information from computer systems and other storage devices (e.g. cellular phones, flash drives, etc.) often requires officers to seize most or all of a computer system or storage media. The computer system or storage media is then typically examined later, by qualified

computer forensic examiners, in a laboratory or other controlled environment. This is necessary because, digital evidence is extremely vulnerable to tampering or destruction. It is also necessary to determine that no security devices are in place that could cause the destruction of the evidence during a search. The search of computer systems and other storage devices is a highly technical process, which requires specific expertise and specialized equipment. There are so many different types of computer hardware and software in use today that it is rarely possible to bring, to the search site, all of the necessary technical manuals and specialized equipment needed to conduct a thorough search.

b) Conducting a search of digital evidence, documenting the search and making evidential copies is a lengthy process. A forensic examination of digital evidence can take weeks to complete depending upon the volume of data stored therein. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to conduct a complete search of the data during the execution of the physical search of the premises. The hard drives, commonly included in desktop computers, are capable of storing millions of pages of text. The storage capacity of other electronic devices (e.g. memory cards, thumb drives, etc.) can also be significant. For instance, a single 100 gigabyte hard-drive is the electronic equivalent of approximately 50,000,000 pages of double-spaced text.

c) Some of the property seized may contain data that is stored in an electronic and machine-readable only format. This data may not be humanly readable in its present state. By this application, I request authorization for searching members to seize, examine, listen to, read, view and maintain the above-described property and to convert it to humanly readable and viewable form as necessary.

d) Computer data, including images of sexual performances by children, written to a hard drive or other storage medium (e.g. DVD's, CD's, memory cards, etc), can be stored for years at little or no cost. Even when such evidence has been deleted, it may be recovered years later using readily-available examination tools. When a person "deletes" data on a hard drive, or other storage medium, the data does not actually disappear; rather, the data remains on the hard drive, or other storage medium, until it is overwritten by new data. Therefore, deleted data or remnants of deleted data, may reside in free space or slack space on a hard drive. Free space or slack space is space on the hard drive, or other storage medium, that has not been allocated to an active file or that has not been used by an active file. In addition, a computer's operating system may also keep a record of deleted data in a "recovery" file. Similarly, files that have been viewed, via the Internet, are usually and automatically downloaded into a temporary Internet directory or "cache". The browser typically maintains a fixed amount of hard drive space devoted to these files and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve these files depends less on when the files were downloaded than on a particular user's operating system, storage capacity, and computer habits.

e) Technology today not only provides Internet access for home computers, but also for cellular telephones, video game systems, etc. Most are now capable of viewing Internet web sites, communicating via e-mail and instant messages, viewing, storing, uploading and downloading of sexual performances of children. Additionally, devices like MP3 players, iPods, digital cameras, cellular phones and digital media storage devices, (e.g. CD's, DVD's, and memory cards) are all capable of storing hundreds to thousands of images of sexual performances of children.

f) It is often necessary to seize certain computer peripheral devices, at the location of the search warrant, in order to later complete an examination of the evidence back at a police station and/or computer forensic laboratory. Some computer peripheral devices, like routers, may also contain evidence material to an investigation:

g) Data storage devices, like compact disks, external hard drives and thumb drives are commonly used by individuals interested in collecting images of child pornography. These individuals use data storage devices in an attempt to avoid detection and/or as a method of "backing up" their collection to prevent from accidental data loss.

h) Computer users can attempt to conceal computer data within digital media storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" are often used as image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal computer data by using encryption, which means that a password or a security device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography". For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

K)

SEARCH METHODOLOGY TO BE EMPLOYED

1. Based upon my knowledge, training and/or experience; and upon consultation with Investigator John Lombardi, a computer forensic examiner with the New York State Police Computer Crime Unit, I know that the search procedures commonly used for investigations involving digital evidence include the following techniques. Your applicant hereby requests authorization to use the following procedures, whether at the location to be searched, listed under Section "B", and/or while in a controlled environment of a law enforcement computer forensic laboratory. This is a non-exclusive list as other examination techniques may be required in order to identify, read, copy and/or document the evidence authorized to be seized under Section "C".

a) On-site imaging of a computer's random access memory ("RAM"). "RAM" is the place in a computer where the operating system, programs and computer data, in use, are kept. This allows the computer to run faster. The on-site collection of "RAM", at a crime scene, can be very important in the digital evidence examination process. A computer's "RAM" may include, but is not limited to, the following: Images containing sexual performances by children, encryption keys for encrypted data, passwords, etc.. Once the computer is unplugged, the information stored in "RAM" may be lost forever because it may not be stored anywhere else on the computer.

b) On-site network connection examination. The on-site examination of a computer network can also be very important in the digital evidence examination process. The examination, of a computer network, may disclose if the computer is connected to the Internet, an internal network or is stand-alone (unconnected to another computer). Network connections may disclose if a computer is connected to a remote storage services (e.g., Dropbox, Google, etc.) or local computer data storage

device (e.g. Network Attached Storage "NAS" devices). A "NAS" can be easily hidden, at a location to be searched, and may only be detectable through the examination of the local computer network.

c) On-site router examination. Routers are used to control access to and/or from other computers on a network. Routers may store important information about the computers, on an internal network, including which computers have obtained access to the Internet via the router. They can reveal the existence of hidden connections, to remote computer data storage locations or other computer devices that are within the physical location being searched.

d) Date/Time accuracy verification. The date and time, on a computer, is maintained on a computer chip known as the complementary metal oxide semiconductor "CMOS". The "CMOS" is located on the computer's motherboard, not on the computer's hard drive. At the time of seizure or imaging, the "CMOS" date and time should be compared to the actual time and any offset should be recorded. An incorrect date and/or time in the "CMOS" might affect the date and/or time stamps of files on the computer's hard drive.

e) Examination of all of the computer data, stored on any seized computer data storage device, to determine whether the computer data falls within the items to be seized, as set forth under paragraph "B".

f) Searching for and attempting to recover any deleted, hidden or encrypted data to determine whether that data falls within the list of items to be seized, as set forth herein. Any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offense, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above.

g) Performing keyword searches through all of the computer data, stored on any seized computer data storage devices. This will determine whether occurrences of specific language, contained in the computer data storage device, exists and are likely related to the crime being investigated.

h) Examining and documenting any counter-forensic applications. Counter-forensic applications are computer programs used to erase or conceal computer data (e.g., Evidence Eliminator, CCleaner, etc). Knowledge of these applications and determination if they have been used, how many times and when they were last run, may give insight into a computer users activities to hide illegal conduct.

L)

STALENESS

1. I further acknowledge that the temporal proximity of this application and the evidence supporting probable cause may arouse the issue of staleness. As such, I tender the following case law and information to support the authorization of this search warrant:

a) Whether the requisite probable cause exists to procure a search warrant is determined by weighing the totality of circumstances.

Illinois v. Gates, 462 U.S. 213 (1983).

b) Evidence supporting probable cause cannot be rejected for staleness as long as there is a reason to believe that those facts are still in existence.
United States v. Beltempo, 675 F.2d 472, 477 (2d Cir. 1982).

c) Courts have repeatedly held that collectors of child pornography often retain their materials, rarely if ever deleting them.
United States v. Cox, 190 F. Supp. 2d 330, 333 (S.D.N.Y. 2002).

d) The observation that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes is supported by common sense and the cases. Since the materials are illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to quickly destroy them. Because of their illegality and the imprimatur of severe social stigma such images carry, collectors will want to secret them in secure places, like a private residence. This proposition is not novel in either state or federal court: pedophiles, preferential child molesters, and child pornography collectors maintain their materials for significant periods of time. The doctrine of staleness applies when information proffered in support of a warrant application is so old that it cast doubt on whether the fruits or evidence of a crime will still be found at a particular location. When determining whether information is stale or not, the judicial officer must not only consider the age of the information, but the nature of the evidence sought. Some kinds of evidence are more evanescent than others. Some contraband, like narcotic drugs, are consumable. Other evidence, like an illegal firearm, is more apt to remain in one place for extended periods. As one court put it, the hare and the tortoise do not disappear at the same rate of speed.
United States v. Lamb, 945 F. Supp. 441, 460 (N.D.N.Y. 1996).

e) It was reasonable to believe child pornography would be found in a suspect's apartment even though ten months had passed since the discovery of evidence supporting the search warrant affidavit. United States Customs agents obtained information that Lacy downloaded six computerized images from a Danish computer bulletin board known to distribute child pornography. Although the agents could only verify that two of the pictures contained child pornography, their information also included the exact time of the call and the names of the files downloaded. Ten months after the transmissions agents executed a search warrant and discovered images of children engaged in sexually explicit activity. Lacy was subsequently convicted on child pornography charges. Denying Lacy's motion to suppress the fruits of the search warrant, the Court held that the probable cause was not stale because, as described in the affidavit, the tendency of child pornography collectors to preserve their collections made it likely that the illicit images would be found in Lacy's apartment, even after the passage of a significant amount of time.
United States v. Lacy, 19 F.3d 742 (9th Cir., 1997), cert denied, 118 S. Ct. 1571 (1998).

f) Information over a year old that relates to child pornography charges is not stale as a matter of law. In July of 2001, Audry Edwards found images of child pornography on the computer of Ernest Newsom, her live-in boyfriend. Although Edwards had moved out, a year later she agreed to watch Newsom's house while he was out of town. While using Newsom's computer Edwards found two video clips of her daughter removing a towel after getting out of the shower. Based primarily on the premise that Newsom likely still had the year old images on his computer, the Lawrence Police Department obtained a search warrant and discovered numerous videos and images of child pornography. Upholding the search warrant, the Court found that "information a year old is not necessarily stale as a matter of law, especially where child pornography is concerned."

Unites States v. Newsom, 402 F.3d 780 (8th Cir., 2005)

g) Notwithstanding the passage of seventeen months, evidence of child pornography was properly included in a search warrant affidavit. Over the course of a fifteen-year relationship, Bateman and an informant exchanged videos and images depicting minors engaged in sexually explicit activity. Although the informant had one subsequent contact with Bateman, February 2001 was the last time he could confirm that Bateman sent him child pornography. Over a year later, on July 16, 1992, the Keene Police Department applied for a warrant and subsequently searched Bateman's home. The police discovered child pornography and charged Bateman with possession of the illicit material. The Court denied Bateman's motion to suppress the evidence found at his home reasoning that "the unique nature of the object of the warrant (child pornography), the unique nature of the creation, storage, keeping, alteration, potential of destruction of the child pornography material, and the recognized interest which the states and the federal government have in drying up the distribution network for child pornography and controlling production itself, are legitimate factors which militate against finding staleness."

United States v. Bateman, 805 F. Supp. 1041 (D.N.H., 1992).

h) Evidence of a transmission of 19 images six months prior to a search warrant application was not stale even though it was the sole verification that the defendant possessed child pornography. A File Transfer Protocol log on an accused child pornography trafficker's computer showed that 19 illicit images had been sent to Alexander Hay on November 29, 1996. On May 28, 1997, United States Customs agents obtained a search warrant based almost exclusively on this information. The only other evidence included in the application simply confirmed that the IP address and computer belonged to Hay. Following his indictment on child pornography charges, Hay moved to suppress this evidence for staleness. In validating the warrant, the Court held that a pattern of activity was not necessary to infer long-term storage of child pornography.

United States v. Hay, 231 F.3d 630 (9th Cir., 2000), cert denied, 534 U.S. 858 (2001).

i) Akin to the federal courts, when child pornography is involved, New York courts have been reluctant to exclude the fruits of a search warrant due to the staleness of probable cause. Evidence supporting the issuance of a warrant to search Manngard's home included facts demonstrating that he had videos and images of children engaged in sexual acts stored on his computer, and an affidavit of an expert in child pornography crimes that explained pedophiles' propensity to retain their collections of illicit materials. Although the Court did not quantify the time-lapse, because the evidence clearly revealed that the defendant was engaged in pedophilia, the probable cause was not stale.

People v. Manngard, 275 A.D.2d 378 (N.Y. App. Div., 2000), leave to appeal denied, 95 N.Y.2d 966 (N.Y., 2000).

j) The Court finds reasonable basis to conclude that a fourteen-month delay between the alleged receipt of child pornography and the search of Defendant's residence did not make the information supporting the warrant too stale to furnish probable cause. This is especially true considering the plethora of case law indicating that substantial time lapses do not invalidate a warrant in child pornography cases. With regards to child pornography, the consensus among courts, including the Fourth Circuit, is that information supporting probable cause is less likely to become stale, even when there exists substantial delays between the receipt of child pornography and the issuance of a search warrant. This consensus is based on the fact that collectors and traders of child pornography share common characteristics that separate said crimes from other criminal acts. In child pornography cases, courts often reject staleness challenges based on widespread expert

opinion that collectors of child pornography store and retain their collections for extended periods of time. Furthermore, Defendant fails to cite, nor is the Court aware of, any cases where a court granted a motion to suppress evidence of child pornography based solely on a finding that the information supporting the warrant was stale.

United

States v. Johnson, 865 F. Supp. 2d 702 - Dist. Court, D. Maryland 2012.

k) Additionally, the ability of forensic examiners to recover files from a computer, even those deleted by a user, impacts a court's staleness analysis. Since evidence on a computer is recoverable months or years after it has been downloaded, deleted, or viewed; the age of the information supporting a warrant is increasingly irrelevant when the object searched is stored on a computer. Thanks to the long memory of computer hard drives, the evidence of a crime is still likely stored on a computer's hard drive, even after a perpetrator tries to delete it.

l) Ultimately, the existence of probable cause is determined by analyzing the totality of circumstances. (Gates). Pedophiles have a proven propensity to retain their collections of child pornography, rarely if ever discarding it. (Lamb). In spite of the fact that there is no hard and fast rule, the federal courts are in seemingly solid agreement that the temporal proximity of child pornography evidence is immaterial to search warrant affidavits. (Lacy), (Newsom), (Bateman), and (Hay). Moreover, that it is unnecessary to show a pattern of activity to bolster the premise that child pornography is often stored for long periods of time. (Hay). In line with federal case law, New York courts have held that evidence of child pornography is capable of negating claims of staleness. (Manngard). In the end, the gap of time between the discovery of the evidence and the application for the search warrant is not given much weight because of the state's recognized interest in eliminating the distribution and production of child pornography, the propensity of child pornography collectors to retain their collection for significant periods of time, and the state's moral obligation to prevent the exploitation of children. (Bateman).

M)

CONCLUSION AND SPECIFIC REQUEST

1. Based upon the above information, your applicant believes that reasonable cause exists to believe that a violation of New York State Penal Law, Section 263.15 and 263.16, has occurred and that evidence of those crimes are currently concealed upon the Person of:

SHANE M. GUAY d.o.b. 05/04/1991, wherever he may be found and

and within the premises known as:

147 NORTH 8TH STREET, OLEAN, NY 14760 – CATTARAUGUS COUNTY, NY

2. Your applicant respectfully requests that the court issue a search warrant authorizing the search of the aforementioned Person and Premises. Furthermore, the search and seizure of the property listed under section "C" for evidence involving the possession and/or promotion of images and/or videos containing sexual performances by children, in violation of New York State Penal Law Section 263.16 and/or 263.15. Your applicant also requests that the search be conducted in the manner requested, under section l, and consistent with the necessary technical requirements needed for the search and seizure of digital evidence.

3. No previous application in this matter has been made in this or any other court or to any other judge, justice or magistrate.

Sworn to before me this

31st day of MAY, 2018.

at 2:30 pm,
In the County of Cattaraugus,
City of Olean,
State of New York.

David R. Palumbo
Applicant

David R. Palumbo
Justice
DAVID R. PALUMBO
OLEAN CITY COURT JUDGE

ATTACHMENT 1

DEFINITIONS

1. Promoting a sexual performance by a child (Penal Law 263.15) – A person is guilty of promoting a sexual performance by a child when, knowing the character and content thereof, he produces, directs or promotes any performance which includes sexual conduct by a child less than seventeen years of age. Promoting a sexual performance by a child is a class D felony.
2. Possessing a sexual performance by a child (Penal Law 263.16) – A person is guilty of possessing a sexual performance by a child when, knowing the character and content thereof, he knowingly has in his possession or control any performance which includes sexual conduct by a child less than sixteen years of age. Possessing a sexual performance by a child is a class E felony.
3. Sexual conduct (Penal Law 263.00(3)) – Means actual or simulated sexual intercourse, oral sexual conduct, anal sexual conduct, sexual bestiality, masturbation, sado-masochistic abuse, or lewd exhibition of the genitals.
4. Use of a child in a sexual performance (Penal Law 263.05) – A person is guilty of use of a child in a sexual performance if knowing the character and content thereof he employs, authorizes or induces a child less than seventeen years of age to engage in a sexual performance or being a parent, legal guardian or custodian of such child, he consents to the participation by such child in a sexual performance. Promoting a sexual performance by a child is a class C felony.
5. Disseminating indecent material to minors in the second degree (Penal Law 235.21(3)) – A person is guilty of disseminating indecent material to minors in the second degree when: Knowing the character and content of the communication which, in whole or in part, depicts actual or simulated nudity, sexual conduct or sado-masochistic abuse, and which is harmful to minors, he intentionally uses any computer communication system allowing the input, output, examination or transfer, of computer data or computer programs from one computer to another, to initiate or engage in such communication with a person who is a minor. Disseminating indecent material to minors in the second degree is a class E felony.
6. Endangering the welfare of a child (Penal Law 260.10 (1)) – A person is guilty of endangering the welfare of a child when: He or she knowingly acts in a manner likely to be injurious to the physical, mental or moral welfare of a child less than seventeen years old or directs or authorizes such child to engage in an occupation involving a substantial risk of danger to his or her life or health. Endangering the welfare of a child is a class A misdemeanor.
7. Computer (Penal Law 156.00(1)) – Means a device or group of devices which, by manipulation of electronic, magnetic, optical or electronic impulses, pursuant to a computer program, can automatically perform arithmetic, logical, storage or retrieval operations with or on computer data, and includes any connected or directly related device, equipment or facility which enables such computer to store, retrieve or communicate to or from a person, another computer or another device the results of computer operations, computer programs or computer data.

8. Computer Data (Penal Law 156.00(3)) – is property and means a representation of information, knowledge, facts, concepts or instructions which are being processed, or have been processed in a computer and may be in any form, including magnetic storage media, punched cards, or stored internally in the memory of the computer.

9. The Internet - is a worldwide network of computers that transmit and receive data by means of using the Internet Protocol ("IP") addressing system. Information and services provided by the use of the Internet Protocol ("IP") addressing system include electronic mail, online chat, file transfer, instant messaging. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

10. Charter Communications - is an "Internet Service Provider", which provides Internet access their customers/subscribers. Charter Communications currently uses both IPv4 and IPv6 to assign internet addresses to their customers/subscribers. Only the first half of the IPv6 address is needed / used by Charter communications to identify a customer/subscriber. The last half of the address is generated by the device using it and is ignored by Charter Communications.

11. Internet Protocol Address "IP" – is an address that a computer uses in order to communicate with other computers on the Internet. Using Internet Protocol Addressing version 4, an "IP" address appears as a series of four groups of numbers separated by dots (i.e. 97.81.148.30). Internet Protocol Version 6 (IPv6) contains (8) blocks of numbers and letters or "hexets" each separated by a colon. An example IPv6 address may look like: F704:0000:0000:0000:3458:79A2:0D8B:4320. The IPv6 addressing allows you use the two-colon (::) shorthand to represent one block full of zeros. Leading zeros can also be omitted. For example, you might abbreviate the IPv6 address above to: F704:::3458:79A2:D8B:4320.

The "IP" addresses assigned to home and/or small business computers are usually obtained from Internet Service Providers "ISP's", like Verizon or Charter Communications. No two subscriber accounts are assigned the same "IP" address at the same time on the Internet. Your home computer's "IP" address can be the same for weeks to months at a time, before being reassigned to another location. Your "IP" address can also change every time your computer connect to the Internet, which may be the case with most "dial-up" Internet accounts. In some cases, IPv6 has the capability to identify a specific device. Some Cellular/wireless service providers are able to use use IPv6 to identify specific subscribers.

12. Download and/or upload - The term "download" means the process of copying computer data from a remote computer data storage device to your own computer data storage device. For example, the act of "downloading" a photo someone "uploaded" to a website to your own computer hard drive. The term "upload" means the process of sending computer data from your computer data storage device to another remote computer data storage device.

13. INSTAGRAM – **Instagram** is an online mobile photo-sharing, video-sharing, and social networking service that enables its users to take pictures and videos, and share them either publicly or privately on the app, as well as through a variety of other social networking platforms, such as Facebook, Twitter, Tumblr, and Flickr. Users can add captions/messages to their uploaded photos/videos and other users viewing those photos/videos can post comments. Instagram users can also engage in private chat conversations with other Instagram users. Instagram Users can add a phone number to their account information. When an Instagram user adds a phone number their

account, Instagram Verifies that number by sending a security code to the number via text message or automated call. The user then enters that security code into the Instagram "verification" box on the application. This process confirms that the Instagram account user has access/control to the "verified" phone number that they provided to Instagram (APP platforms verification etc. Instagram is owned by Facebook and legal requests and releases of Records occur through Facebook.

14. Data Storage Devices - Data storage devices are defined as a device used for the purpose of storing computer data. Data storage devices include, but are not limited to, internal and/or external hard disk drives, floppy disks, compact disks, digital video disks, magnetic tapes, thumb drives, memory cards, media cards, sim-cards, zip drives and RAM and/or ROM units.

15. Curtilage - (As per Cornell University Law School) includes the area immediately surrounding a dwelling, and it counts as part of the home for many legal purposes, including searches and many self-defense laws. When considering whether something is in a dwelling's curtilage, courts consider four factors:

- a. The proximity of the thing to the dwelling;
- b. Whether the thing is within an enclosure surrounding the home;
- c. What the thing is used for.
- d. What steps, if any, the resident took to protect the thing from observation/ access by people passing by.

The Supreme Court suggested these factors in the context of determining whether or not a barn was part of a house's curtilage. See United States v. Dunn (1987), 480 U.S. 294.

In the context of criminal procedure, courts generally call any part of the property surrounding a dwelling that is not part of the curtilage an "open field".

16. Malware - Short for "malicious software", malware refers to software designed to damage or do unwanted actions on a computer system. Common examples include viruses, worms, Trojan horses and spyware.

17. ARIN.net - "American Registry for Internet Numbers", a nonprofit member-based organization, supports the operation of the Internet through the management of Internet number resources throughout its service region; coordinates the development of policies by the community for the management of Internet Protocol number resources; and advances the Internet through informational outreach.

18. Metadata - A general term used to describe the additional descriptive data that is stored along with file content is "Metadata". A simple way to describe "Metadata" is that it is "Data" about "Data" - For example: A Microsoft Word document readily displays the text of a document to a user. That text is stored in the file in the form of data. What is not readily visible to a user, but is available in a Word document file is additional data that contains information about that document and its contents. Some, but not all of the Metadata that can be found by viewing the "properties" tab of a Word document are: Author, Company, number of words, number of pages and the dates and times the document was created, modified, accessed and printed.

19. Exif Data - Digital Images captured with most modern digital cameras contain metadata that adheres to an industry standard called, EXIF (Exchangeable Image File Format). EXIF, also known as EXIF Data contains information about a digital image that may include, but is not limited to: the make, model and serial number of the camera used to take the picture, the date and time the picture was taken, the GPS coordinates of where a picture was taken, the distance from the camera to the subject and with some cameras, the name of the owner of the camera. Digital Video captured with a digital camera does not generally adhere to an industry standard, but may contain metadata that may include, but is not limited to: the make and model of the camera used to record the video, the GPS coordinates of where the video was taken and recording settings.

20. Cellular phone - A cellular telephone is a handheld wireless device primarily used for communication through radio signals. Cellular phones send signals through networks of transmitter and receivers called "cells". This enables communication with other cellular telephones or traditional "land line" telephones. Cellular phones usually store "call logs", which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, most cellular phones offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text, photo and video messages and email; taking and storing photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Cellular phones may also include global positioning system ("GPS") technology for determining and recording the location of the device.

21. Mobile Device - The term Mobile Device, is often used interchangeably with the term cellular device or cellular telephone. Devices other than a dedicated cellular telephone can also be considered to be a mobile device and can function in the same or similar manner as a cellular telephone. Many tablets have a SIM card slot and are capable of connecting to the internet through a cellular network. Certain applications will allow a Tablet or other SIM enabled device to make "voice" "phone" calls and send and receive text messages while using a cellular based internet connection.

22. Verizon Wireless "NATTING" Router IP Address - Verizon Wireless uses Routers and Network Address Translation (NAT) as part of the process which enables Verizon Wireless Customers to use Verizon's cellular service to access the internet from their Mobile Devices. This process allows multiple Verizon Wireless customers to use the same External IP address to simultaneously access the internet. During this usage, Verizon Wireless records information/data regarding the Customer's Internet Session/Connection period during a specified Time and Date. Some of the recorded information includes:

- a) The Subscriber Number (Cellular "Phone" Number).
- b) The "NATTING" IP address (External IP address used by the user to connect to the Internet)
- c) Session Start and End Times. (Also known as Port Allocation and Port Deallocation Dates and Times).
- d) The Outgoing Port Number and Ending Port Number. (Also known as Block Start and Block End)

e) Mobile IP Address (Private IP address assigned to the user during the specified Time Period)

Depending on the individual investigation, some or all of the above information may be used to aid in the identification of a customer/person who was using Verizon Wireless to access the internet from a specific IP address, during a specified Time or Time period.

23. Memory Card - A memory card, sometimes known as "MicroSD" memory cards, are designed to store computer data. A majority of cellular phones in use today have the capability to use "MicroSD" memory cards as attached and removable computer data storage.

24. Cloud Storage - Cloud Storage is remote data storage that is available to users over a network or the internet. Certain devices and applications routinely use "cloud storage" to back up important data, such as pictures, videos, documents etc. Cloud storage can also be used to store backups of entire devices. Cloud storage and certain Applications also allow users to automatically "Synchronize" data across multiple devices and platforms.

25. Sim Card - A Subscriber Identity Module (i.e. "SIM") is a smartcard that is inserted into some cellular devices. The "SIM" card contains a cellular network user's subscriber profile and allows a cellular device to access cellular networks. A "SIM" card may contain a cellular device user's contact list, "text" messages in addition to other computer data. In some cases, the SIM card's primary function is to allow the Cellular device and/or mobile device to access the internet through the cellular network.

26. (MDN) - Mobile Directory Number - The number dialed to reach a user on a CDMA Cellular network. (PTN) - Personal Telephone Number can also be used to describe a user's cellular telephone number.

27. (IMEI) - International Mobile Equipment Identity (Identifier) - a factory-installed unique serial number that identifies a Mobile Device.

28. (MEID) - Mobile Equipment Identity (Identifier) - similar to an ESN; it is a globally unique number that identifies a mobile Device.

29. (ESN) - Electronic Serial Number - A unique number that identifies a mobile Device. Sometimes referred to as a (MSN) - Mobile Serial Number.

30. (MSID) - Mobile Station Identification Number - A 10-digit unique number that a wireless carrier uses to identify a mobile phone. This number may or may not be the same as the (MDN) for a given device.

31. (IMSI) - International Mobile Subscriber Identity - A unique identification number associated with GSM, UMTS and LTE network users. The (IMSI) is stored in the SIM card.

32. (NAI) - Network Access Identifier - Network Access Identifier for a Sprint (CDMA) device. It is similar to an email address. (Example: jondoe1@123.com). The NAI is only available on Sprint (CDMA) handsets. The NAI will end with @sprintpcs.com.

33. Instant Messaging - ("IM") - **Instant** messaging is a form of communication that uses text based messages between two or more participants over a computer network. This type of technology is commonly used by cellular phone users, but may also be used on desktop and/or laptop computers. There are many different applications, in use today, that use this technology. The applications include: iMessage, Kik, Instagram, Skype, etc. Some of these programs allow images and/or videos to be sent and received by other parties. The messages are usually stored within the program, for later reference, and are usually retrievable through a digital device examination.

34. Child Erotica - For the purposes of investigations involving the possession and/or promotion of a sexual performance by a child and/or investigations involving the sexual abuse of children, child erotica refers to materials that sexualize children and/ or materials or items that are likely to be sexually arousing to persons having a sexual interest in children. These materials may consist of:

- a. Images and/or Video that depict children in sexually suggestive poses, engaging in sexually suggestive activities or wearing sexually suggestive clothing or lack thereof.
- b. Images and/or Video, such as animated video, "comic books" and drawings that depict children in sexually suggestive poses, engaging in sexually suggestive activities, wearing sexually suggestive clothing or lack thereof or engaging in sexual conduct.
- c. Images and/or Video of what appear to be adults, that have been edited to appear as a child (often a child's head on an adult body) that depict children in sexually suggestive poses, engaging in sexually suggestive activities, wearing sexually suggestive clothing or lack thereof or engaging in sexual conduct.
- d. Stories, narratives or descriptions that describe children in a sexually suggestive manner or describe children engaging in sexual conduct.

35. UTC - Many of the time and date stamps in found in digital evidence contain references to "Coordinated Universal Time". You will often see the abbreviation for "Coordinated Universal Time" as (UTC) or (UTC +0) next to a time and date reference.

For the period from March 13, 2016 to November 6, 2016 Daylight Saving Time was in effect for the Eastern Time Zone. Eastern Daylight time (EDT) is 4 hours behind Coordinated Universal Time (UTC) and can be obtained by subtracting 4 hours from UTC times/dates for this period.

For the period from November 06, 2016 to March 12, 2017 Standard Time was in effect for the Eastern Time Zone. Eastern Standard Time (EST) is 5 hours behind Coordinated Universal Time (UTC) and can be obtained by subtracting 5 hours from UTC times/dates for this period.

4/17/2018

Instagram video and inappropriate conversations with a 12 year old - w.sturdevant@harriscountysheriff.org - Harris County GA Sheriff's Office Mail

Instagram video, and inappropriate conversations with a 12 year old

inbox x


 W Sturdevant <w.sturdevant@harriscountysheriff.org>
to burtonfan1991

4:46 PM (17 hours ago)

I am an investigator with the Harris County Georgia Sheriff's Office. I have tracked down your email, name and other information via your IP address on Iels68belfrinds. I would like to speak with you in reference to a case I am working. My phone number is 706-628-9400 ext 205. At this point an time i am not looking to lake charges I want to be clear this conversation with my victim is over. I need to hear from you by the end of the week. I thank you for your time and would like to get this cleared up as soon as possible.

Investigator W.P. Sturdevant 1-7

shane guay
to me

4:48 PM (17 hours ago)

I have deleted everything social media wise. Anything that has happened is over with. I was going through rough times and was saying things that were stupid. It was a massive mistake and I regret it.



DEPARTMENT OF HOMELAND SECURITY

HOMELAND SECURITY INVESTIGATIONS

REPORT OF INVESTIGATION

OFFICIAL USE ONLY | LAW ENFORCEMENT SENSITIVE



11/14/2018 13:06 EST

Page 2 of 3

DETAILS OF INVESTIGATION

On August 6, 2018, Homeland Security Investigations (HSI) Buffalo Special Agents (SA) Nicholas Melchiorre and John Kosich met with New York State Police (NYSP) Investigator (Inv) John Lombardi and Senior Inv. Scott Folster at the NYSP Troop A Headquarters in Batavia, NY to take custody of 26 pieces of evidence seized from the residence of Shane GUAY (COC: USA DOB: 5/4 /1991) located at 147 N 8th Street, Olean, NY on June 5, 2018 pursuant to a New York State search warrant.

Inv. Lombardi released the following 26 items of evidence to SA Melchiorre via NYS form A421, lab case 18TA-00044, Dept. Case #7558239 dated 8/6/18:

AGENT NOTE: NYSP evidence was labeled items 2-27. SA Melchiorre relabeled the evidence 001-026 when seized and annotated the evidence number changes on all evidence bags and HSI chains of custody.

- LG cellular phone Model: VS-988, IMEI: 355273084799554
- Sony PlayStation 4
- Acer Aspire laptop, serial number 03450966816
- Compaq Presario laptop, serial number 1V24KQ49942G
- Compaq Presario computer tower, serial number MXK418PW3
- Dell Dimension computer tower, serial number DJPQM31
- Gateway computer tower, serial number 0019334218
- E-Machines computer tower, serial number QLM2490023838
- Dell Inspiron laptop computer, service ticket #6536C91
- Compaq Presario laptop, 5CB2057WYH
- Xbox 360 gaming system, serial number 408022520505
- Sony PS3 (damaged), serial number AA313325609-CECH-4001B
- Acer Aspire laptop, serial number LUSDE0B005041459DA1601
- Coby 512 MB Media Player
- Samsung cellular phone (serial number not identified)
- Go Pro Digital Camera with 32 GB micro CD card
- Sandisk 16 GB Flash Media Thumbdrive and Dsnap media player
- LG cellular phone (serial number not identified)
- Sony Play Station Portable (serial number not identified)
- Sony Playstation 2 with controller (no power cable)
- Xbox 360 gaming system, serial number 608958654025 (no power cable)
- Apple iPod 8 GB and Apple iPod 1 GB
- Samsung cellular phone, model SCH-U450

Current Case Title

Shane GUAY

ROI Number

BU07QS18BU0025-006

Date Approved

8/22/2018

OFFICIAL USE ONLY | LAW ENFORCEMENT SENSITIVE

This document is loaned to you for official use only and remains the property of the Department of Homeland Security. Any further request for disclosure of this document or information contained herein should be referred to HSI Headquarters together with a copy of the document.